UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

vs. Case No. 07-CR-171

DAVID SZYMUSZKIEWICZ,

Defendant.

BRIEF SUPPORTING
DEFENDANT'S MOTION FOR ACQUITTAL

At both the close of the government's case and the close of evidence, defendant David Szymuszkiewicz moved for a judgment of acquittal. The Court took the motion under advisement. David now files this brief in support of that motion.

THE CHARGE AND THE INSTRUCTIONS

David is charged with three counts of intentionally intercepting electronic transmissions by use of a device in violation of 18 U.S.C. §2511(1)(a). The jury was instructed that to convict David, it must find that he intercepted an electronic communication and that he did so intentionally. The jury was further

instructed that to "intercept" means "to acquire the contents of any electronic communication by using any electronic, mechanical or other device."

Historically, section 2511(1)(a) has been used to prosecute persons who used a device, such as a wiretap, to secretly and contemporaneously intercept the telephone conversations of another. More recently, prosecutors have used the statute to prosecute computer hackers and email thieves. However, there is no reported decision involving the facts of this case, where the government charged a passive recipient of emails that were forwarded to the defendant by a rule created on the sender's computer. This is an issue of first impression.

THE UNDISPUTED FACTS

The following facts were stated during trial testimony and are undisputed.

Revenue officers and supervisors from the Milwaukee area offices of the Internal Revenue Service are issued laptop computers and have been utilizing them since approximately 2000. IRS laptop computers are password protected and lock down after fifteen minutes of inactivity. Once that lock down or sleep mode occurs, the user must re-enter the assigned password in order to be able to perform any functions.

IRS employees use Microsoft Outlook for both internal and external electronic communications. All email communications to and from IRS employees in the Midwest, including to employees whose offices are located in

Southeast Wisconsin, are received and stored on an exchange server located in Kansas City, Missouri. When employees' computers are online, *i.e.*, connected to the IRS network, email communications are received from and sent to the Kansas City exchange server.

Microsoft Outlook rules that are created to forward email communications also are created and maintained on the Kansas City exchange server. Such communications are not accessible if an individual computer is disconnected from the exchange server or is off-line.

Forwarding of email communications is very common within the Southeastern Wisconsin offices of the IRS. In addition to Outlook forwarding rules, IRS employees also utilize distribution lists and delegated access to allow electronic communications to reach secondary recipients.

David is a revenue officer who, until 2007, was assigned to the Racine office of the IRS. Nell Infusino is a retired group manager who was David's supervisor from the late 1990s to approximately 2004-05. Although based in different office locations, at various times over the years, David and Infusino have worked in the same office. However, David has never had access to Infusino's password, nor was there any evidence that he has used Infusino's computer at any time when it was connected to the IRS network.

It is policy for IRS group managers to designate acting managers to act in their stead during periods in which the manager is unavailable. David has served as acting group manager for Infusino on several occasions from 2000-2005.

In April 2006, Infusino found a rule in Outlook that stated the following:

> "Apply this rule after the message arrives. . . where my name is in the to or cc box, forward it to Szymuskiewicz, David S."

The rule was deleted on the date of discovery and no longer exists. No evidence exists to indicate who created the rule, or when it was created.

A search of David's laptop and the IRS exchange server recovered approximately 130 emails "auto-forwarded by rule" from Infusino to David between February 2003 and April 2006. Infusino and David both deny creating the rule. David and Karen Kammers state that Infusino was aware of emails she auto-forwarded to David. Infusino denies any such knowledge.

ARGUMENT

In a motion for judgment of acquittal, the question is "whether the record contained sufficient evidence from which the jury could reasonably find the defendant guilty beyond a reasonable doubt." *United States v. Swan*, 486 F.3d 260, 266 (7th Cir. 2007) (quoting *United States v. Theodospoulos,* 48 F.3d 1438, 1444 (7th Cir. 1995). The evidence is viewed in the light most favorable to the government, recognizing that it is the jury's function to determine witness

credibility and to draw *reasonable* inferences. *Id.* The court's role in reviewing the verdict is to determine whether the government has presented evidence on every element of its case sufficient for the jury to have found the defendant guilty beyond a reasonable doubt. *United States v. Marquardt,* 786 F.2d 771, 780 (7th Cir. 1986). The government failed to meet that burden in this case.

I. THE GOVERNMENT FAILED TO PROVE AN "INTERCEPTION" AS THAT TERM IS DEFINED IN SECTION 2511.

There is no dispute that emails were forwarded to David's computer via a rule created on the computer of IRS revenue officer Infusino. However, it is not enough for the government to prove that David received the emails. The statute requires the government to prove, by evidence beyond a reasonable doubt, that David intentionally intercepted the emails, meaning that he used an "electronic, mechanical or other device" to deliberately and purposefully access those emails. In addition, the emails must have been intercepted simultaneous to their transmission, as opposed to having been obtained from electronic storage. The government's failure to prove these facts mandates a judgment of acquittal.

A. The Government Did Not Produce Any Evidence That David Used An Electronic, Mechanical Or Other Device To Intercept The Emails.

Section 2511 unequivocally requires proof that a defendant intercepted an electronic communication through defendant's use of "an electronic, mechanical

or other device." The government did not present any evidence that David used such a device to intentionally, *i.e.* deliberately and purposefully, cause Infusino's emails to be forwarded to him. The government argued that the "device" that was used was the computer on which the forwarding rule was created. Courts that have interpreted section 2511 have uniformly rejected similar arguments, instead mandating the use of a device separate and distinct from a computer, its drive or its server.

In *Crowley v. Cybersource Corporation*, 166 F.Supp.2d 1263 (C.D. Cal. 2001), the court dismissed an amended complaint that alleged violation of the Federal Wiretap Act, 18 U.S.C. §§2510-2521, also known as Title I of the Electronic Communications Privacy Act. The court stated that there was no "interception" as that term is defined in the Act: "Amazon did not, however, 'intercept' the communication within the meaning of the Wiretap Act, because Amazon did not acquire it using a device *other than the drive or server on which the e-mail was received*." *Crowley*, 166 F.Supp.2d at 1269. The court then added that holding Amazon liable for merely receiving an email

> would be akin to holding that one who picks up a telephone to receive a call has intercepted a communication and must seek safety in an exemption to the Wiretap Act. Such a result would effectively remove from the definition of intercept the requirement that the acquisition be through a "device."

Id. The court granted the defendant's motion to dismiss the claim under the Act. *Id*.

The Eastern District of Pennsylvania relied on *Crowley* in dismissing a complaint's Wiretap Act allegations in *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, (E.D. Pa. Dec. 13, 2007). There, the plaintiff, Ideal, had hired some former employees and purchased some assets of a bankrupt non-party company Carco, but lost a bid to purchase the company outright to the defendant, Acutronic. Thereafter, emails sent by third parties and some of Ideal's employees, including former Carco employees, to email addresses containing the Carco domain name, were received on the Carco servers and were automatically forwarded to Acutronic. *Id.* at *4. The court rejected Ideal's argument that the forwarding of the emails violated section 2511(1)(a), stating that Ideal had failed to allege the use of a device to intercept the communications. *Id*. The court then cited *Crowley* for its holding that "the drive or server on which an e-mail is received does not constitute a device for purposes of the Wiretap Act." *Id*. (citing *Crowley*, at 1269).

The government here did not prove or even attempt to prove that David used any "electronic, mechanical or other device" to intercept Infusino's emails. As in *Crowley*, there has been no allegation that David acquired the emails by using any device "other than the drive or server on which the e-mail was

received." *Crowley*, 166 F.Supp.2d at 1269. Indeed, the government's theory was that David, at some unknown time, secretly accessed Infusino's computer and, thereby, accessed the IRS's Kansas City server, in order to create a rule forwarding Infusino's emails to himself via the same server.

By failing to present any evidence that David used some device other than the existing IRS computer and server system to intercept the emails, the government failed to prove an "interception" as that term is defined under the Wiretap Act. The government's failure to prove this element of the offense mandates entry of a judgment of acquittal.

B. The Government Did Not Establish That The Emails Were Intercepted Contemporaneously With Being Sent.

In 1986, Congress amended the Federal Wiretap Act to create the Electronic Communications Protection Acts, establishing two distinct subparts: Title I, which has continued to be referred to as the Wiretap Act, governed intercepted communications; and Title II, named the Stored Communications Act (SCA), which governs access to stored -- as opposed to intercepted -- communications and records. *See* Pub. L. No. 99-508, 100 Stat. 1848; 18 U.S.C. §2701(a). Several Courts of Appeals have considered the interplay between the two provisions, reaching the inescapable conclusion that a violation of the Wiretap Act occurs only where the communication is acquired contemporaneous with its original transmission.

One of the earliest courts to address this issue was the Fifth Circuit in *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), holding that the government's acquisition of email messages that were stored on an electronic bulletin board system, but not yet retrieved by the intended recipients, did not constitute an "interception" under the Wiretap Act. The court noted its prior interpretation of the word "intercept" to mean acquisition of a communication contemporaneous with its transmission, *see United States v. Turk,* 526 F.2d 654, 658 (5th Cir.), *cert. denied,* 429 U.S. 823 (1976), and Congress's stated intent to retain that definition "intercept" in expanding the Act to cover interceptions of electronic communications. *Steve Jackson*, 36 F.3d at 460, 462. The court then noted the distinct definitions of wire and electronic communications under the Act, whereby "wire communications" were defined to include stored information while "electronic communication" was not.

> Critical to the issue before us is the fact that, unlike the definition of "wire communication," the definition of "electronic communication" does not include electronic storage of such communications.... Congress' use of the word "transfer" in the definition of "electronic communication," and its omission in that definition of the phrase "any electronic storage of such communication" ... reflects that Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage."

Id. at 461-62.

After *Steve Jackson*, several district court opinions adopted its reasoning, including: *Wesley Oil v. Pitts*, 974 F.Supp. 375, 386 (D. Del. 1997) ("[B]y including the electronic storage of wire communications within the definition of such communications but declining to do the same for electronic communications . . . Congress sufficiently evinced its intent to make acquisitions of electronic communications unlawful under the Wiretap Act *only if they occur contemporaneously with their transmissions*."), *aff'd,* 172 F.3d 861 (3d Cir. 1998) (emphasis added); *United States v. Reyes*, 922 F.Supp. 818, 836 (S.D. N.Y. 1996) ("Taken together, the definitions thus imply a requirement that the acquisition of [electronic communications] be *simultaneous* with the original transmission of the data.") (emphasis added); and *Bohach v. City of Reno*, 932 F.Supp. 1232, 1236-37 (D. Nev. 1996) (requiring acquisition during transmission).

The Ninth Circuit endorsed the reasoning of *Steve Jackson Games* in *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998). The issue in *Smith* was whether the Wiretap Act covered not only wire communications in transmission, but also wire communications in storage, such as voicemail messages. The *Smith* court, relying on the *Steve Jackson Games* analysis that the definition of wire transmissions, including communications in storage, agreed that wire communications in storage could be "intercepted" under the Wiretap Act. *Id.* at

1057. The *Smith* court added that the more limited definition of "intercept" applied to electronic communications:

> [I]n cases concerning "electronic communications" - the definition of which specifically includes "transfers" and specifically excludes "storage" - the "narrow" definition of "intercept" fits like a glove; it is natural to except non-contemporaneous retrievals from the scope of the Wiretap Act. In fact, a number of courts adopting the narrow interpretation of "interception" have specifically premised their decisions to do so on the distinction between §2510's definitions of wire and electronic communications.

Id. (citations omitted). As a result, the court agreed with the defendant's argument that a third-party's retrieval and recording of voicemail messages was "interception" in violation of the Wiretap Act and affirmed the trial court's order suppressing that evidence in Smith's criminal trial. *Id*. at 1058.

Perhaps because of *Smith* and similar rulings, in 2001's USA Patriot Act, Congress amended the Wiretap Act to eliminate the reference to "storage" from the definition of wire communications under the Wiretap Act. The purpose of the amendment was to reduce protection for voicemail messages to the same level as other electronic communications. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002), *cert. denied,* 537 U.S. 1193 (2003) (citing H.R. Rep. 107-236(I), at 158-59 (2001)). "By eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of 'intercept' -- acquisition contemporaneous with transmission -- with respect to wire communications." *Id*. (citing *Smith,* 155 F.3d at 1057 n.11). In other words,

because Congress was aware of the narrower judicial interpretation of the term "intercept" as applied to electronic communications when it amended the statute to apply the same definition to wire communications such as voicemail messages, "Congress, therefore, accepted and implicitly approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission." *Id.* Based on this analysis, the *Konop* court concluded: "We therefore hold that for [an electronic communication] to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage." *Id.*

Other courts have reached the same conclusion. *See In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003); *Fraser v. Nationwide Mutual Ins. Co.*, 352 F.3d 107 (3d Cir. 2003); *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003); *Bailey v. Bailey*, 2008 WL 324156 (E.D. Mich. Feb. 06, 2008); *United States v. Moriarty*, 962 F.Supp. 217, 221 (D. Mass. 1997) (recognizing difference between Wire Tap Act, governing acquisition of contents of electronic communications contemporaneous with transmissions of those communications, and Stored Communications Act, which governs once electronic messages are stored.);

The same analysis must apply here. Emails sent to Infusino's computer were not intercepted by David's computer contemporaneous to the original transmission of the emails. Instead, after the emails were transmitted to and received by Infusino, her computer then routed the emails back through the IRS

server in Kansas City, and that server then forwarded the emails to David's computer. The very language of the rule in question confirms that is only applied "after the message arrives." The process that occurred here did not involve contemporaneous interception and therefore does not meet the long held definition of intercept under the Wiretap Act. Because the government presented no evidence that David acquired the emails contemporaneously with their original transmission, it failed to prove the element of interception. David therefore requests entry of a judgment of acquittal.

II. EVEN IF THE STATUTORY DEFINITION OF INTERCEPTION INCLUDES AUTO-FORWARDED EMAILS, THE GOVERNMENT DID NOT PROVE THAT DAVID INTENTIONALLY VIOLATED SECTION 2511(1)(a).

Even if this Court disagrees with the caselaw cited above and determines that causing emails to be auto-forwarded pursuant to a rule constitutes an "interception" under section 2511(1)(a), entry of a judgment of acquittal is still required because the evidence was insufficient to establish that David intentionally caused the interception. David cannot be convicted of violating section 2511 absent evidence beyond a reasonable doubt that he intentionally intercepted the emails. To prove intent, the government must establish that David acted deliberately and purposefully. At best, the government's evidence as to intent amounted to nothing more than speculation and conjecture, and a conviction based on speculation and conjecture cannot stand. *See United States v.*

Howard, 179 F.3d 539, 542 (7th Cir. 1999) (judgment of acquittal should be granted where evidence is "so scant that the jury could only speculate as to the defendant's guilt, and a reasonably minded jury must have had a reasonable doubt as to the defendant's guilt") (citing *United States v. Fearn*, 589 F.2d 1316, 1320-21 (7th Cir. 1978)).

The only evidence submitted regarding David's intent is that the forwarded emails were received by David. The government argued that the jury could infer from that fact to reach the conclusion that David somehow accessed Infusino's computer and created the auto-forwarding rule. However, the government never examined Infusino's computer or her exchange server repository of electronic communications to determine when or how the rule was created. The government did not present any witness who rebutted David's testimony that he has never used or acquired any knowledge regarding Outlook rules. The government seized his laptop, but found no evidence that the Outlook "rules and alerts" feature had ever been utilized. No evidence was offered that David had the skill or capacity either to access Infusino's computer or to create a rule. David's testimony that he had never used or had any knowledge regarding Outlook rules stands unrefuted.

In *Wesley College*, the College sued an employee and faculty members, alleging a violation of section 2511(1)(a). A compromise in security in the

College's email system resulted in the defendants' receipt of communications intended for other recipients. In assessing the College's claim, the Delaware District Court first stated that "[l]iability under this aspect of Title I, is predicated, then, on an affirmative attempt by the Defendant to intercept, or persuade another to intercept, an electronic communication." *Wesley College*, 974 F.Supp. at 381. In other words, liability could not be predicated solely upon passive receipt of the emails.

The College attempted to create a basis for the court to draw the inference that the defendants had intentionally acted to intercept the emails, relying on the alleged motive that the defendants stood to benefit by having received communications. The College offered several scenarios through which it might have been possible for the recipients to have intentionally intercepted the emails. The court, however, rejected the College's conjecture, stating that neither scenario was supported "by a shred of admissible evidence." *Id.* at 381-82. The court stated:

The *Wesley College* Court characterized the College's claim and the evidence it found insufficient to survive summary judgment as follows:

> At bottom, a factfinder would be asked to determine liability on the above bases from three things: (1) motive (2) an apparent discrepancy in the testimony of Pitts and Ferguson, and (3) emails sent to Stewart through campus mail which nobody has of yet owned up to. This is not enough; a reasonable factfinder could not conclude, without more, that either Ferguson or Hudson took

> affirmative steps to intercept or access Stewart's e-mail when there is no evidence they possessed the capability to take those steps or joined forces with somebody who did.

Id. at 382.

The court ultimately granted summary judgment to the defendants, finding a complete failure of proof of any intentional affirmative acts. *Id*. at 392.

Similarly, the evidence presented by the government was not enough for a reasonable factfinder to conclude that David intentionally and purposefully created or caused someone else to create an auto-forward rule on Infusino's computer. Based solely on the existence of the rule, the government asked the jury to infer the following facts, without presenting any testimony or other evidence:

1. David, at some unknown place and time, accessed Infusino's computer while it was in active mode.

2. David had an understanding and the ability to create rules through Microsoft Outlook.

3. David secretly created the rule, despite the fact that he replied to Infusino's forwarded emails, thus alerting her that messages had been auto-forwarded to him.

The government failed to elicit any testimony necessary to prove these facts.

Although drawing reasonable inferences is permitted, this Court should not allow the jury to fill in the gaping holes in the government's evidence through guesswork and conjecture. As the Seventh Circuit stated in reversing in

part a conviction arising from an alleged conspiracy, "[s]upposition will not suffice." *United States v. CEA,* 914 F.2d 881, 888 (7th Cir. 1990); *See also United States v. Black*, 2007 WL 3254452 *11 (N.D. Ill. Nov. 05, 2007) (granting judgment of acquittal on indicted count because the "thin reed of evidence" presented by the government amounted to speculation) (citing *United States v. Moore,* 115 F.3d 1348, 1364 (7th Cir. 1997) (conviction cannot rest upon speculation or conjecture)); *United States v. Browne,* 225 F.2d 751, 756-57 (7th Cir. 1955) (reversed mail fraud conviction where only testimony regarding use of the mails was speculative and the government's own witness testified "against an inference that it was received through the mails").

The sole evidence regarding intent was that the rule forwarded emails to David. No one saw David create an auto-forward rule on Infusino's computer. The government produced no evidence as to when the rule was created. David was denied any ability to investigate the creation of the rule because the rule was allegedly deleted after discovery, and any trace of it was erased from the server. Moreover, although proof of motive was not required, the only motive the government volunteered was that David was "nosy" and, inexplicably, that he lost his driver's license more than a year after the first known auto-forwarding by rule.

David recognizes that he faces a large hurdle in requesting a judgment of acquittal based on the insufficiency of the government's evidence; however, this is one of the rare cases where such relief is justified. The government's case was predicated solely on the assumption that because the emails were auto-forwarded to David's computer, then he must have created the rule. If that level of conjecture is allowed, then every person who ever possesses stolen property is guilty of burglary or theft. Moreover, although it was the only party with access to and control over the server and computer in question, the government chose not to investigate Infusino's computer usage and her past practices to determine whether its assumption was controverted by historical fact.

Even under the light most favorable to the verdict, the government utterly failed to prove that David intentionally intercepted Infusino's evidence through use of a device. A judgment of acquittal should be entered.

III. IF THERE WAS ANY CONFUSION AS TO WHAT THE GOVERNMENT WAS REQUIRED TO PROVE, THE RULE OF LENITY MANDATES A JUDGMENT OF ACQUITTAL.

If this Court determines that the definition of "interception" under the Wiretap Act is ambiguous as to whether either (1) the computer on which an auto-forward rule is created is a "device" under the statute or (2) acquisition of an email via an auto-forward rule is contemporaneous with the email's transmission, then this Court should apply the Rule of Lenity. The Rule of

Lenity "insists that ambiguity in criminal legislation be read against the prosecutor, lest the judiciary create, in common-law fashion, offenses that have never received legislative approbation, and about which adequate notice has not been given to those who might be ensnared." *United States v. Thompson*, 484 F.3d 877, 881 (7th Cir. 2007) (citing *Staples v. United States,* 511 U.S. 600, 619 n.17 (1994)).

The Wiretap Act, as written and as judicially interpreted, does not provide citizens fair notice that receiving forwarded emails could be construed as violative of the Act. All prior constructions and interpretations of the Act required use of a separate device, acquisition of the communication contemporaneous to its transmission, and an affirmative act indicating an intent to intercept. Due Process is offended by any new construction of section 2511 that retroactively declares David's past conduct to be criminal. Thus, the Rule of Lenity mandates entry of a judgment of acquittal.

CONCLUSION

For all the foregoing reasons, the government did not prove that David Szymuszkiewicz committed the offense of intentionally intercepting electronic communications through use of a device. David respectfully urges this Court to enter a judgment of acquittal as to all three counts of the indictment.

Dated this 17th day of October, 2008.

GIMBEL, REILLY, GUERIN & BROWN

By:
/s/Patrick J. Knight
PATRICK J. KNIGHT
State Bar No. 1013374
KATHRYN A. KEPPEL
State Bar No. 1005149
Attorneys for Defendant

POST OFFICE ADDRESS:

Two Plaza East, Suite 1170
330 East Kilbourn Avenue
Milwaukee, Wisconsin 53202
Telephone: 414/271-1440
R:\Criminal\Szymuszkiewicz, David\Pleadings\acquittalbrief10-16-08.doc